DIALOGUE

Drones and Environmental Monitoring

Summary

Aerial drones are emerging as an effective tool for environmental monitoring and enforcement because of their ability to reach areas that would be otherwise inaccessible or cost-prohibitive. However, the regulatory framework has not developed as fast as the technology, raising concerns. As EPA and other agencies consider using drones to monitor industrial sites and farmland, many landowners claim it would be an invasion of privacy. Using drones for inspections also raises legal questions about information obtained from drone flyovers and the associated evidentiary requirements. Fraught with legal uncertainty and significant public interest, the use of drones for environmental monitoring and enforcement raises important questions for many stakeholders. On August 30, 2016, ELI convened a panel to discuss drone use and regulation. Below, we present a transcript of the discussion, which has been edited for style, clarity, and space considerations.

Joanna Simon (moderator) is an Associate with Morrison & Foerster LLP.
Amanda Essex is an Attorney and Policy Associate with the National Conference of State Legislatures.
Joseph Muhlhausen is the co-founder of CielMap.
Jeramie Scott is the National Security Counsel for the Electronic Privacy Information Center.

Joanna Simon: As an Associate with Morrison & Foerster LLP, my practice started out in traditional aviation, doing liability work for big parts manufacturers, specifically avionic manufacturers. Over the past two to three years, it has largely transitioned into an unmanned aircraft systems (UAS) practice—so, I'm excited to talk to you all about drones.

On the panel, we have Amanda Essex, who is an Attorney and Policy Associate in the Transportation Program at the National Conference of State Legislatures (NCSL). She has worked for NCSL since 2013, joining the transportation program in December 2014. There, she researches, writes, and presents on a range of topics that includes UAS.

Next, we have Joseph Muhlhausen. He is the co-founder of CielMap, a geospatial data analysis company with a focus on environmental mapping, monitoring, and risk assessment. He is a remote-sensing specialist with many years of experience in the environmental and sustainable development applications of satellite images. He will give us some insights specifically into environmental issues, sensing, and the types of technologies that might go into that.

We also have Jeramie Scott, who is the National Security Counsel and Privacy Coalition Coordinator for the Electronic Privacy Control Center (EPIC). His work focuses on privacy issues implicated by domestic surveillance programs that use drones, biometrics, big data, and license plate readers. He also runs monthly privacy coalition meetings that bring together representatives from consumer and privacy organizations with key Washington, D.C., decisionmakers in the privacy field.

The focus of my presentation is on Part 107 of the Federal Aviation Regulations,[1] which is the new small UAS regulation that became effective August 29, 2016. Before we do a deep dive into Part 107, I'd like to start with where we are as a society—how the rest of the people in the country use drones—not just people who are using them for an official or business purpose.

The reason it's important to consider how drones are viewed in popular culture is that society is really driving how FAA is going to regulate drone activity. We have to think about what pressures are facing the agency as they move forward with regulation. There are many beneficial uses for drones, which include solar and infrastructure monitoring. Then, there are well-known uses in the film and agriculture industries. Delivery of packages and even people may be possible at some point. Of course, environmental uses are a big portion of what this might include, such as pipeline monitoring, emergency preparedness, and conservation.

You now have a better idea about what we do. We have represented a wide variety of drone clients, ranging from the manufacturers, to service providers, to Facebook in their high-altitude platform, to The Nature Conservancy (TNC), which you see at the forefront in using drones for conservation. They have all really pushed FAA to develop rules that make sense for their usage.

1. Operation and Certification of Small Unmanned Aircraft Systems, 14 C.F.R. Part 107 (2016).

The bottom line is that FAA views drones as aircraft and, thus, aircraft rules are going to apply. No one can operate a drone in the national airspace without specific authorization from FAA. In 2012, the FAA Modernization and Reform Act (FMRA)[2] was passed, which tasked FAA with developing a plan for the safe integration of drones into national airspace. FMRA required FAA to draft a final rule integrating small drones by August 2014. Obviously, August 2014 came and went, and there was no small drones rule, but hopefully we are now on our way.

In the interim, between 2014 and when the small drones rule became effective in 2016, we had the "§333 Exemption." It was named for FMRA §333, which allowed FAA to authorize what it determined were safe uses of drones in advance of a final rule. Many of you might have §333 Exemptions. They became fairly commonplace over the past couple of years, with a set of standard conditions that apply: you need a pilot's license; you need to operate at relatively slow speeds; no higher than 400 feet above ground level; and the drone must stay in visual line of sight of the operator.

I want to talk about §333 Exemptions because not only did it lay the groundwork for what became the small drones rule, but you also now have an option to continue to operate under a §333 Exemption, if you choose to do so. Most §333 Exemptions are good for a period of two years from the time they are issued, and since most were issued in the past year, they will last until 2017 or 2018. A §333 Exemption might enable you to perform slightly more extensive operations than would be possible under Part 107 without seeking a waiver. So, it is important to take a good hard look at what your §333 Exemption allows you to do when making the decision to continue operating under a §333 Exemption or start operating under Part 107. It is important to note that you must choose to operate under either §333 or Part 107—you cannot conduct an operation under both.

Part 107 was issued in June 2016 and became effective on August 29, 2016. The operational limitations of UAS under Part 107 are actually very similar to what we see in §333, for the most part: less than 55 pounds; a visual line of sight; no flying above uninvolved people; daylight operation only; a maximum speed of 87 knots; one-UAS-to-one-pilot ratio, meaning a pilot cannot operate more than one drone at a time; no operations from a moving vehicle; and a maximum altitude of 400 feet above ground level or within 400 feet of a structure. For example, if you are trying to inspect a building, you do not need to be within 400 feet from the ground if the building rises above 400 feet. You can be within 400 feet of the ceiling of that building. You can operate in Class G airspace, which basically requires no permission from air traffic control (ATC). In other classes, you will need to request ATC permission. You may also transport property for hire if your total weight is less than 55 pounds, meaning the drone and its payload, and you can stay within visual line of sight and not operate from a moving vehicle.

Perhaps the most useful part of Part 107, as opposed to §333, is that it establishes a remote pilot in command position and allows you to get a UAS certification. In order to do so, you will need to pass an initial aeronautical knowledge test vetted by the Transportation Security Administration. You must be at least 16 years old and comply with registration requirements. The Part 107 certificate will also impose reporting obligations. Pilots will have 10 days to report an accident or an incident if serious injury occurs, if there is loss of consciousness, or there is property damage of $500 or more. Additionally, the Part 107 reporting obligation to FAA is separate and apart from reporting obligations that exist to the National Transportation Safety Board, which are outlined in different sets of regulations. So, you will want to be cognizant of the fact that there might be dual reporting obligations and this might not encompass everything that must be reported to each agency.

One of the most important sections of Part 107 is its waiver provision—this is what distinguishes Part 107 from a §333 Exemption. Essentially, any operational requirement or limitation under Part 107 can be waived. The operation from a moving vehicle, you can get that waived. You can waive the requirement for operations to be conducted only in daylight. You can get a visual line-of-sight requirement waived, and you can get the new UAS-to-pilot ratio waived. You can also get the other operating limitations on speed and altitude waived.

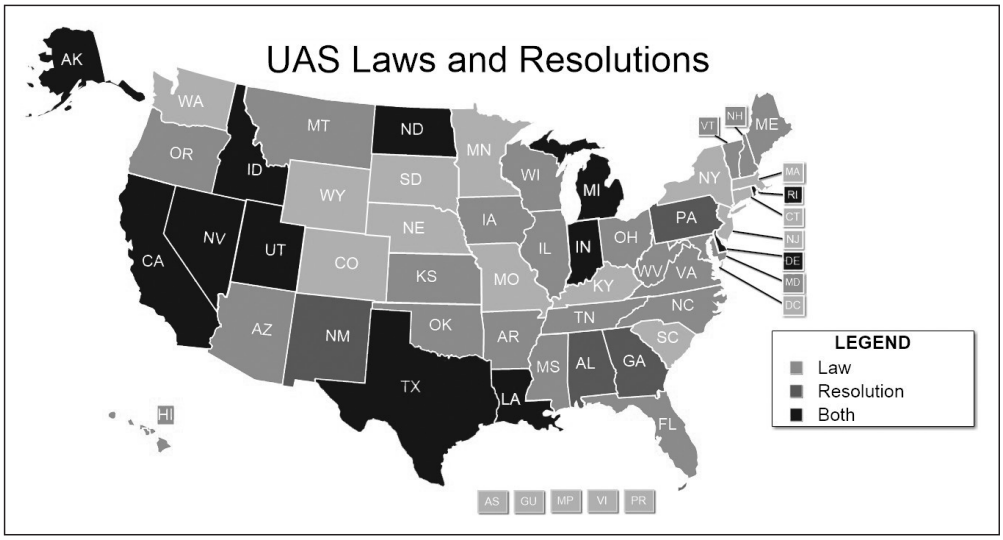
This waiver provision was created largely in response to comments that FAA received regarding the notice of proposed rulemaking. We worked with TNC to ask for less-restricted daytime operations and visual line-of-sight requirements, because those provisions have tended to hamper conservation efforts. We view drones as a critical conservation tool and they would not be able to be used in the ways that would provide the most value without the waiver option. FAA took comments by TNC and other entities into account when writing the final rule. It had a huge impact on the rulemaking process and developed what is arguably the most important part of Part 107. This is something to keep in mind for your business—when other drone rulemaking efforts occur—if your mission profile is not going to be accommodated, you should always consider commenting and encouraging the agency to adopt a flexible approach, because they are usually willing to do so if and when it makes sense, and if there is a safety case for it.

There are also other options for drone use in businesses. These are much more difficult to achieve, such as the special airworthiness certificate, which is highly restricted. Practically speaking, they are not always available or given at the discretion of FAA. So, it is not that we cannot do it, but that it is going to take a lot of work and an iterative process between your company and the agency to

2. Pub. L. No. 112-95, 126 Stat. 11 (Feb. 2012). For further discussion of FMRA and other legal and constitutional issues surrounding drone use, see Lucase Satterlee, *Climate Drones: A New Tool for Oil and Gas Air Emission Monitoring*, 46 ELR 11069 (Dec. 2016).

work together with the right data packages to approve your safety case. Once you have your airworthiness certificate, you're going to be a lot less restricted but in tight collaboration on what you can do.

What is next? Part 107 is not a comprehensive regulation mandated by FMRA §332. It was actually promulgated under §333 just like through the exemptions. Basically, they are taking incremental steps to integrate drones into national airspace. Future §332 regulations are likely to address operations not currently authorized right now under Part 107 autonomous operations, beyond visual line-of-sight operations, and even perhaps beyond radio line-of-sight operations. We will need to have more secure technology, with a certain level of encryption for command and control. Overall, it is important that no doors are closed and that the pace of change is currently accelerating.



Amanda Essex: Thank you, Joanna. I'm a policy associate in the transportation program at the NCSL. For those who are not aware of NCSL, we are a nonprofit and bipartisan organization. We serve all 50 state legislatures, including all 7,383 legislators and more than 30,000 legislative staff. We have offices in Washington, D.C., and Denver. We provide information and research on a wide range of policy issues, including UAS. I'm going to provide a brief overview of the national legislative landscape as it relates to the topic of UAS, also known as drones or unmanned aerial vehicles. Then, I will discuss federal preemption of state drone laws, trends seen in UAS legislation over the past few years, and wrap up with state preemption of local regulations.

FAA is tasked with regulating the national airspace; therefore, actions taken by the agency affect state legislative policy. It's very important to consider federal action on UAS, because any state laws that directly conflict with FAA regulation will be invalidated under the principle of preemption. In December 2015, FAA released a fact sheet on state and local regulations,[3] specifying what the agency believed were appropriate areas of legislation for states, including regulations in areas typically related to state and local police powers. This includes land use, zoning, privacy, trespass, and law enforcement operations. The fact sheet also recommended that governments consult with FAA before they legislate in certain areas, particularly any regulation of the national airspace. At one point, the U.S. Senate's FAA reauthorization legislation included language that would have broadly granted state legislative action on UAS, but this language was ultimately left out of the final legislation.

Now that we have explored federal preemption, let us take a look at what states have been doing to regulate UAS. I am going to start with some numbers. Since 2013, between 35 and 45 states have considered legislation on drones each session. In 2013, 13 states enacted 16 new laws. In 2014, 10 states enacted 11 new laws. Then, in 2015, we saw 26 new laws in 20 states. That year, Virginia's governor also signed an executive order related to drones.[4] By August 30, 2016, at least 38 states had considered legislation and 15 states had enacted 28 new laws. At some point in the past three years, every state but South Dakota has considered legislation related to drones.

As of August 2016, 32 states have enacted laws related to drones. With so many states involved in drone legislation, we have been able to identify a number of trends. One area where states have been particularly active in legislation involves privacy concerns. Twenty-two states have laws addressing privacy, with 18 states requiring law enforcement to obtain a warrant before they use UAS to collect evidence or conduct surveillance, and at least four states require that the use of drones by law enforcement be reported. Twelve states have laws intended to address privacy violations committed by other citizens. For example, in Arkansas, certain uses of drones were added to the definition of voyeurism and video voyeurism,[5] and Mississippi prohibits using a drone to commit "Peeping Tom" activities.[6]

Another emerging issue related to drones is the requirement that operators have insurance. To my knowledge, no state has yet passed a law requiring insurance. But in 2015, Florida and New Jersey both considered legislation regarding the appropriate amount of liability insurance for drone

3. Federal Aviation Administration, *State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet* (Dec. 17, 2015), *available at* https://www.faa.gov/uas/resources/uas_regulations_policy/media/uas_fact_sheet_final.pdf.

4. Exec. Order No. 43 (June 12, 2015), *available at* https://governor.virginia.gov/newsroom/newsarticle?articleId=8593.

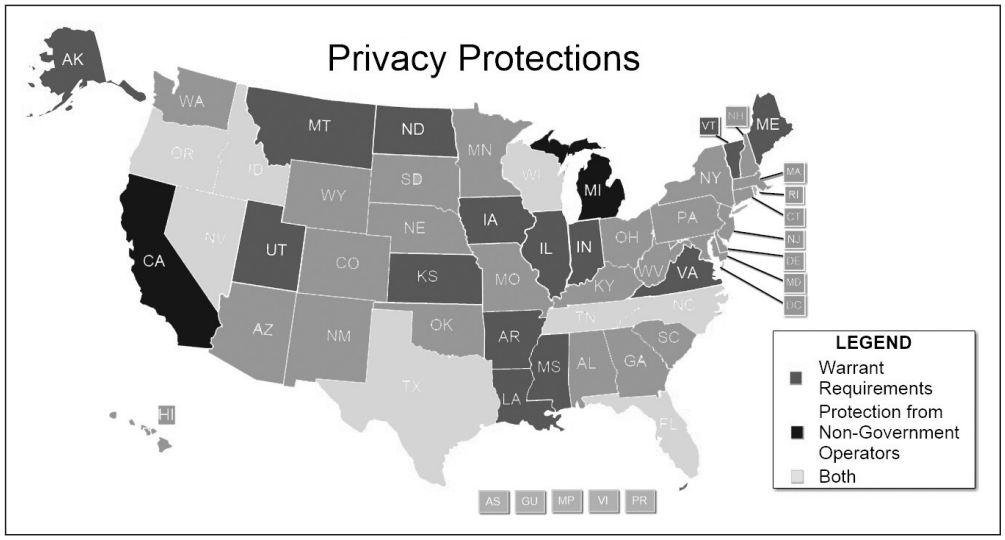
5. Ark. H.B. 1349 (2015).

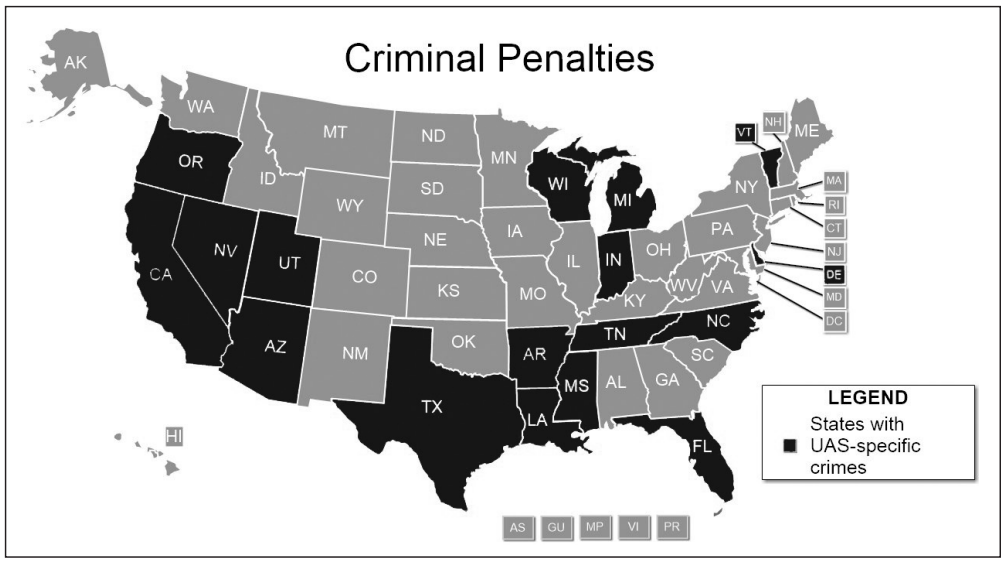
6. Miss. S.B. 2022 (2015).

operators. In 2016, at least three more states considered whether insurance needs to be mandated for UAS operators.

Many states have recognized the great commercial potential of this technology. It is important to note that commercial use of UAS is regulated, first and foremost, by FAA through Part 107, but some states have also taken action to regulate or explicitly authorize commercial operations. For example, Florida has a general prohibition on using drones to capture images of privately owned properties without permission, but they include exemptions for a number of commercial uses, including environmental monitoring.[7]

States have also recognized the many potential governmental uses of UAS. Legislation has specifically allowed the use of this technology for photographing traffic crashes and crime scenes. Virginia allows the use of drones when certain alerts have been issued, such as an AMBER alert.[8] Some state laws also allow the use of drones for aerial photography to assess floods, fires, and other storm damage, and to determine if a state of emergency needs to be declared. Laws in Tennessee[9] and Texas[10] allow the use of drones to conduct air quality sampling and for fire suppression, and states' departments of transportation have been using drones for infrastructure maintenance, including bridge and road inspections.





Lawmakers have also considered addressing criminal behavior related to UAS. Fifteen states have laws specifically criminalizing certain uses of drones. Indiana includes a prohibition on unlawful photography and surveillance of private property with a UAS.[11] In Louisiana, unlawful use of UAS consists of surveilling a targeted facility without the owners' prior written consent.[12] North Carolina criminalized a number of actions, including using a drone to interfere with manned aircraft, possession of a weaponized drone, and operating commercially without a license.[13] In 2016, Utah criminalized operating a drone within certain distances of a wildfire.[14] The state enacted a law on this topic in early 2016 and enacted another bill in a special session in July that increased the criminal penalties for newly established crimes.

While a number of states have taken action criminalizing certain behaviors, there continues to be debate as to whether these laws are necessary. In California, three laws passed both chambers in 2015 that would have criminalized operating drones over wildfires, correctional facilities, and schools. However, all three of these bills were vetoed by the governor. In his veto message, Gov. Jerry Brown stated that, "each of these bills creates a new crime—usually by finding a novel way to characterize and criminalize conduct that is already prescribed. This multiplication and particularization of criminal behavior creates increasing complexity without commensurate benefit."[15] His veto

7. Fla. S.B. 766 (2015).
8. Va. H.B. 2012 (2013); Va. S.B. 1331 (2013).
9. Tenn. S.B. 1892 (2014).
10. Tex. H.B. 912 (2013).
11. Ind. H.B. 1009 (2014).
12. La. H.B. 1029 (2014).
13. N.C. S.B. 744 (2014).
14. Utah H.B. 126 (2016).
15. Veto Letter from Gov. Edmund G. "Jerry" Brown to the California Assembly (Oct. 3, 2015), *available at* https://www.gov.ca.gov/docs/AB_849_Veto_

message really went to the argument that new laws might not be necessary when there are already laws on the books that might address these behaviors.

Another issue related to criminalization that has been getting some news coverage recently relates to weaponization of drones. You may have heard the story about the young man in Connecticut who attached a gun to his drone and fired it while in the air, and then subsequently posted a video on YouTube of him attaching a flamethrower to his drone in an attempt to roast a turkey for Thanksgiving. These videos and the subsequent news coverage have prompted more states to consider legislation on weaponization. Eight states have laws on this issue; three of those states prohibit the use of weaponized drones by law enforcement in public bodies, although in North Dakota the law specifically prohibits lethal weapons, which has raised the question about the use of non-lethal weapons such as tear gas and tasers.[16] Five other states say that no one can possess or use a weaponized drone.

Another early trend relates to the way UAS can impact hunting and fishing. Six states prohibit the use of drones for hunting and/or fishing, and seven states prohibit using a drone to interfere with others who are lawfully hunting and fishing. Three states explicitly prohibit both.

Restricting operations near critical infrastructure is another emerging trend. A handful of states prohibit using drones near critical infrastructure such as petroleum refineries, nuclear facilities, and chemical and rubber manufacturing facilities. However, generally these restrictions do not apply when the operator has the permission of the facility owner.

States have also looked at restricting the operation of drones near or around prisons. In 2015, there were a handful of news stories about drones dropping contraband, including tobacco, marijuana, and heroin, into a prison yard. Six states prohibit the operation of drones near or over correctional facilities. Additionally, Texas has a law that requires developing rules to address the use of drones in the capitol complex, and a number of states have regulations that limit operating drones near state capitol buildings.[17] At least 13 states have created a task force on drones or requested a report or study in order to further evaluate the implications of this technology in their state.

Federal preemption is not the only type of preemption that needs to be considered when it comes to drones. States have also looked at legislation that preempts local laws. Arizona,[18] Oregon,[19] Maryland,[20] Rhode Island,[21] and Virginia[22] all have laws specifying that only the state can make laws and regulations on UAS. One of the primary goals of these laws is to avoid a patchwork of regulation at the local level and to develop consistency for drone operators in the state. NCSL released a comprehensive report on state UAS legislation, *Taking Off: State Unmanned Aircraft Systems Policies*, in June 2016 that includes all of this information and much more, and is available for free on the NCSL website.[23]

Joseph Muhlhausen: Thank you, Amanda. I'm going to talk about my company and the kind of applications we do with drones. I'm going to quickly talk about Part 107—it has been extensively covered—and define aerial systems of drones for environmental applications, give our industry perspective, and then provide a quick case study that we did in the Marshall Islands in March 2016.

At CielMap, we have very extensive expertise in remote sensing. We have worked with all different kinds of sensors: satellite, airborne sensors, and drone sensors. We have worked on soil erosion risk, deforestation, urban expansion, and so on. We are located in Maryland, but we mostly work internationally. Our unique expertise is using drones for flood modeling and our results are very close to the gold standard of remote sensing, which is Light Detection and Ranging (LIDAR). LIDAR is a laser imaging system used for topography mapping. Our accuracy is within the margin of error of LIDAR, and we are one of the few companies to have achieved this and are very proud of that.

Part 107 changes everything for us, because it reduces the regulatory burden. You no longer need to be a private pilot licensed to fly a drone. Now, there is easier access to becoming a drone operator or drone pilot within the national airspace. You don't need to take practice lessons, just a knowledge test. We have started looking at new projects that we could do, having some restrictions waived, such as flights over or near populated areas.

Moving on to drones for environmental purposes, there are two main types. First, you have multicopters, they take off vertically and, like helicopters, they can hover around. They can fly for about 10 to 30 minutes and carry a small payload. Second, there are fixed-wing devices, like planes, which can cover more ground, but also need more space for takeoff and landing. In general, fixed-wing devices can cover about 100 to 1,000 acres and can fly at 15 to 25 knots. They weigh around five pounds and fly for about 30 minutes to an hour. In terms of payloads, it can be something as simple as a point-and-shoot camera to very advanced imaging systems such as LIDAR, radar, gas, or temperature or pressure sensors. The main limitations on payloads are usually weight and volume. Obviously, a drone cannot carry a very heavy payload.

One of the main issues in geospatial applications of drones for environmental purposes is that there are already tools available, and they all have advantages and disadvantages. For example, satellites may be more cost-effective if

Message.pdf.
16. N.D. H.B. 1328 (2015).
17. Tex. H.B. 3628 (2015).
18. Ariz. S.B. 1449 (2016).
19. Or. H.B. 2710 (2013).
20. Md. S.B. 370 (2015).
21. R.I. H.B. 7511 (2016); R.I. S.B. 3099 (2016).
22. Va. H.B. 412 (2016).
23. Amanda Essex, *Taking Off: State Unmanned Aircraft Systems Policies* (2016), National Conference of State Legislatures, *available at* http://www.ncsl.org/research/transportation/taking-off-state-unmanned-aircraft-systems-policies.aspx.

you cover a large area. The question is, are drones a replacement for those tools or are they new and additional tools? I would argue that drones are an additional tool, yet revolutionary when used at the right scale and for the right purpose. The right scale may be when you need a highly detailed small coverage of about 100 to 1,000 acres or you need to make multiple flights, such as once a day or every hour, and it is within line of sight due to regulations.

There are many different examples of environmental applications of drones; one example is monitoring. Let's say that you want to monitor the algae bloom in a lake daily, then you need to do multiple data collections, which is the strength of drones. For planning, if you want to map invasive species for land use assessment or land area, let's say in the Midwest, you won't be able to detect those invasive species most of the time using satellites. Drones can detect that in a small area. You can use a geostatistical model to combine both data sets for your planning purposes and map invasive species in large areas. You can also use drones for monetizing. Many small-scale projects will become economically viable using drones. One can think of biomass estimates of forests transformed into carbon credits. Then, finally, enforcement drones can be deployed really quickly. During an inspection, someone can just carry a drone in a suitcase to fly over the area. If there is a contaminant spill, they can be deployed within a few minutes of the event.

Let's move to the case studies. Last March, we worked in the Marshall Islands, which is located in the middle of the Pacific Ocean. It is a group of 33 low-lying atolls, the highest elevation point is only 10 feet, and they are sadly threatened by sea-level rise. We went to the island of Wotho, which is about two hours away from the main island. Its area is about 3 square kilometers, or 1.5 square miles. There are 145 people living on the island. This is one of the strengths or one of the advantages of using drones: for a small population, it would have been too expensive to charter a plane with sensors all the way to the Marshall Islands. Satellites don't provide enough details to properly and with high accuracy map such islands; therefore, drones are the most effective tools.

It took us about two hours to map Wotho. The three-dimensional model of the island looks very flat because it's low-lying. Our goal was to map flood risk and see how the population would be affected in the event of a flood. The model shows a one-meter sea-level rise with a storm surge and different scenarios of low to high tide—from a best-case to a worst-case scenario. Best case would be plus 2 meters, and the worst case plus 3.5 meters. Even in the best-case scenario, the airstrip on the island is flooded, so no deliveries of emergency supplies or evacuations of people could take place. In the worst-case scenario, the whole populated area of the island is flooded. So, this map will help the Marshallese government make preemptive plans to evacuate the population before a storm.

In conclusion, I would say that drones are not going to replace some of the other existing tools, but they are a new tool. They have the potential to revolutionize environmental applications when used at the right scale and for the right purpose, and I would argue that Part 107 allows for it to happen in a timely manner in the United States.

Jeramie Scott: I am the national security counsel at EPIC, a D.C.-based public interest research center. It focuses on emerging privacy issues, and I focus on a bunch of different domestic surveillance issues, including drones, specifically. EPIC's involvement with this issue actually predates FMRA, when we did a Freedom of Information Act request with respect to the use of drones by the U.S. Department of Homeland Security's Customs and Border Protection Agency.

Once FMRA was passed, we actually petitioned FAA to conduct a notice-and-comment rulemaking on the privacy and civil liberties impact of domestic drone use. There were a number of organizations and experts who signed on to the petition that went to FAA. It took a while, but FAA eventually responded, years later, and basically said that they weren't going to do a separate rulemaking on the privacy issues related to drones. However, they said that they would consider privacy in the context of their upcoming small drone rulemaking, which was the one in the early part of 2015, and consider the rules for line-of-sight drones under 55 pounds.

Of course, when the small drones rulemaking came out, and the notice for it soliciting comments, it actually ended up saying that privacy was outside the scope of that particular rulemaking. That is when EPIC filed suit against FAA, arguing that its decision to exclude privacy issues from the drone rulemaking and to deny EPIC's petition was arbitrary and capricious. In that case, the U.S. Court of Appeals for the District of Columbia (D.C.) Circuit ruled that we had to wait until the rulemaking had been completed before filing suit, so the case was temporarily dropped. But since the rulemaking has been completed, we recently filed against FAA in the D.C. Circuit again with respect to privacy and domestic drone use.

During this time, the president released the Presidential Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems.[24] A large focus of this memo was on the government's use of drones, but it also requested that the National Telecommunication and Information Administration and the U.S. Department of Commerce conduct a multistakeholder process to come up with volunteer rules for the use of drones in the commercial context. It is something that we thought was, and is, inadequate to address the privacy issues associated with drones.

There has also been some research done by the Pew Research Center that gives perspective on people's views of the use of domestic drones. In the 2014 survey, it showed

24. Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

that 63% of Americans think it would be a change for the worse if personal and commercial drones were given permission to fly through most of U.S. airspace.[25] In the 2015 survey, they found that 74% of Americans believe control over personal information is very important, but only 9% believe they have such control.[26]

These are important things to keep in mind, because many people see drones as a threat to their privacy in ways that other technologies haven't been. Whether this is true or not, we see it play out in real life in terms of people's perspectives and actions. Some of you may be familiar with the Kentucky case, in which a man shot down his neighbor's drone as it was flying over his property.[27] The judge ruled in favor of the man who shot down the drone. Just recently, there was another case where a woman in Virginia shot down a drone over her property with a 20-gauge shotgun.[28] In both instances, these people cited privacy concerns as what was on their minds when they saw the drones hovering over their property.

I tend to lump the use of drones into three large categories: recreational/hobby, government, and commercial. EPIC tends to focus on the latter two, government and commercial drone use, although there are definitely privacy issues with recreational drone use, as well. Particularly, it allows people to use it for voyeurism and to be "Peeping Toms." As we previously heard, there are some state laws covering that, although it is still an issue that probably needs to be further addressed, since drones make it easier to commit these types of crimes.

Our focus is more on commercial drone use, which is expected to rise—somewhere in the area of 600,000 commercial drones are anticipated over the next year or so. They will be used in aerial photography, filmmaking, inspections, and environmental monitoring. There are actually many privacy issues raised by the commercial use of drones, even in the context of environmental monitoring, although there are less privacy risks in that context than in situations where you have drones flying over people constantly. You can imagine a scenario when the technology advances enough or when we have the "Amazons" and "Googles" flying drones to deliver packages, which will travel over very populated areas. Privacy risks increase a lot more in that context.

That is because drones pose a unique threat to privacy. The technical and economic limitations to aerial surveillance changed dramatically with the advancement of drone technology. The surveillance capabilities of drones are rapidly advancing and cheap storage is readily available to maintain repositories of the surveillance data. The combination of these factors will make pervasive and indiscriminate aerial surveillance feasible.

Technologies that our drones already have include, obviously, high-definition cameras and infrared cameras. The ability to put facial recognition or license plate recognition software on drones is possible. You can also place cell phone tower simulators, also known as stingrays, in drones that will basically act like a cell tower to collect all cell signals and location data for cell phones in the area. A couple years ago, a marketing firm in Los Angeles actually tested a drone in Los Angeles to collect cell phone location data. They are able to do this because cell phones constantly emit wireless probes to find local networks to connect to. Those probes include a unique number known as a media access control address. That unique identifier is just some of the information that drones have the capability to collect. Understand that technology only continues to advance and become more accessible as prices drop, and these are privacy-invasive technologies.

In the case of using drones for environmental monitoring, as I mentioned, the risks are lower, but you still need to be wary of those risks, particularly if you're anywhere people might be present. The drones may not have the capability to do facial recognition, but can still identify human forms using cell phone signals to access how many people are in the area. Also, drones used for monitoring traffic may be using license plate readers to identify the number of unique cars going through a particular area.

It's important to be wary of those particular issues in order to make people comfortable with the implementation of domestic drones. This also includes addressing the security issue, which is something I don't think drone makers have focused on too much. Most drones aren't particularly hard to hack at this point, and you don't want a scenario where either someone can take over the drone with all this high-tech equipment on it or can access the data the drone has collected.

Finally, based on the survey results we saw earlier from Pew, I think the burden is really going to be on the industry to make people comfortable with the implementation of drones, and that means addressing the privacy risk with domestic drone integration. Part of the key to that is going to be transparency in a few different forms: transparency in terms of the surveillance equipment on the drone; transparency with respect to the information being collected by the drone; and transparency of where drones are flying and when.

Drones are also not easily identifiable right now. FAA only requires the drone to be registered and the registration number to be on the drone at some point. But since they are very small vehicles, that a lot of times can fly high enough that you might not even notice them, it is really hard to identify a drone that you think is operating inappropriately. I had a recent experience with this out on a lake

25. Aaron Smith, *U.S. Views of Technology and the Future*, Pew Research Center (Apr. 17, 2014), http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/.
26. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, Pew Research Center (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.
27. *Judge Dismisses Charges for Man Who Shot Down Drone*, WDRB.com (Oct. 26, 2016), http://www.wdrb.com/story/30354128/judge-dismisses-charges-for-man-who-shot-down-drone.
28. Cyrus Farivar, *Woman Shoots Drone: "It Hovered for a Second and I Blasted It to Smithereens,"* Ars Technica (Aug. 29, 2016), http://arstechnica.com/tech-policy/2016/08/65-year-old-woman-takes-out-drone-over-her-virginia-property-with-one-shot/.

with some friends in a boat. We actually had a drone fly over us and follow us for a while. There was probably someone on the mainland videotaping us with this drone and it was a little unnerving. There was nothing we could do about it or way we could identify who was using the drone. I didn't have a gun to shoot it down. Not that I would have, but that option wasn't available to me.

So, with the capabilities of drones in terms of aerial surveillance, with the drop in price and increase in technology, it is going to be really important to address these issues upfront. To give a parallel, we don't want a situation like with cookies in web browsing. Cookies came about with consumers and users unaware that all this information collection was going on as they searched the web. Only more recently were people made fully aware of all the information that can be collected in this way. I think that type of situation probably won't happen in this context, with drones flying around collecting a bunch of information with people unaware or disinterested in what's going on, because drones are a hot topic. Because of that, and in order for the integration to go smoothly, I think industries are going to have to be very proactive about addressing these privacy risks going forward.

Questions & Answers

Joanna Simon: I wanted to start with a question for Jeramie. Are there particular privacy concerns that might come up in the environmental monitoring context? It's been said that drones are really just a platform for a camera or for a sensor, and so you're going to be collecting all types of data. Not just the data that you actually are going to be using for your particular purpose. What are the privacy concerns with that? Also, are there particular best practices that a company could put in place in order to make sure that its data is secure?

Jeramie Scott: Sure. As I mentioned before, the privacy risks in the environmental context are lower, because a lot of that use is going to happen where there's not a lot of people around. However, there will be instances where there is going to be monitoring of people, whether you're flying over a piece of property with houses, such as in the context of providing video for a seller to promote or sell a piece of property or house in a neighborhood. In those situations, you just have to be aware of the people around you and whether your drone has the type of technology that might collect information on those people.

Obviously, high-definition cameras are going to collect images of people if they are in the area you are flying over. But if you're monitoring traffic and you have a license plate reader in addition to a high-definition camera, or things of that nature, those are the kind of things that raise privacy concerns. People don't want their information collected without their knowledge or consent. Although you don't have the same type of privacy rights in public, there is still a certain amount of expectation of privacy in public. The expectation of privacy in public is something that I think is going to come to a head in the next few years, because there is a growing number of technologies that collect or can collect information on people.

In order to be proactive in addressing this issue, transparency in enforcement and public accountability will be key. With respect to security, it's going to be important to start using encryption, where it isn't already being used, in two ways: (1) encryption of the communication line between the controller of the drone and the drone itself, to prevent someone from taking control of a drone or accessing its surveillance equipment; and (2) encryption is also needed with respect to the data that is collected. These two aspects of security are going to be important moving forward and depending on the type of data being collected, the security should be higher the more sensitive the information.

Joanna Simon: Thanks very much for that. We also received a question asking whether you have to have permission from landowners in order to fly over their land under Part 107. I think this question can be broken into two parts. If it's just the land, the answer is likely no. But Part 107 does restrict operations over people who are not involved in the operation. So, if you're going to be flying over someone else's land and there are people below you who are not involved in your particular operation, that use is going to be restricted under Part 107.

As a practical matter, in the context of environmental monitoring, when you need to fly over a portion of private land in order to get to what you're looking at, it's usually best, in going to Jeramie's point about transparency, to just ask and explain what you're doing—that you're not going to be capturing images of people or you're not going to be looking at their house. A lot of times, when people have knowledge of what's actually going on, they don't mind the operation. It is the lack of transparency, when someone just sees something flying over them or over their land, that makes people upset or piques their interest in what's going on. People are generally more open to technology when they are kept informed.

I also wanted to shoot a question over to Amanda. Have you seen particular state laws that might have an impact on specifically environmental uses of drones?

Amanda Essex: There has been a little bit of state action in that. For the most part, it is within the commercial use regulations that states have enacted, but I think it's been fairly limited. As I mentioned before, I think it was Florida that has something specific to environmental monitoring. There are a few other states that have talked about allowing different uses, but when it comes to regulating commercial use, the states have been fairly limited in their action, and I think for the most part this would be considered commercial use. There are a handful of states that maybe have something: Florida, Louisiana, Maryland, North Carolina, possibly; and, as I mentioned, Tennessee and Texas both have some regulation. So, those are the states that could

be impacted at this point by enacted laws when it comes to environmental monitoring.

Joanna Simon: Thanks. Our next question is for Joseph. When it comes to your uses of drones, how do you engage with the particular population—local people or local agencies—when you are going to conduct an operation to monitor a particular piece of land? Are there best practices that you have in place in order to alleviate concerns and to alleviate any particular regulatory burden on your operation?

Joseph Muhlhausen: Yes. We make sure we have the landowner's permission, obviously. We also ask people around the landowner for permission, as well. We usually invite people to see the drone, to learn how it works and how it acquires data. I think that's the most reassuring part of it. It allows them to kind of take ownership of the technology. We will also show people the results we get, if they are interested and the client is willing to share some of the data. It is usually best to talk about the fact that you need to fly over a piece of land beforehand—at the beginning of the contract, not a day before—because if concerns are raised, it is better to address them early on.

Joanna Simon: Thanks very much. We have another question that came in for Amanda. Is there any interest among states in developing model legislation that would not only harmonize laws across state lines, but also consolidate laws within states?

Amanda Essex: There has definitely been discussion of the development of model legislation, but, as far as I know, there hasn't been anything developed yet. I have spoken with someone who indicated that they were going to be putting together a working group to develop something. NCSL itself does not craft model legislation. In the report that I mentioned earlier, we tried to bring together all of the information so that everyone—all the legislators and staff—knows what other states are doing.

Joanna Simon: I think this is a really great question, not just for purposes of the United States, but in terms of international drone operation. There is an entity at the United Nations called the International Civil Aviation Organization (ICAO), and they are developing standards and recommended practices for drone operations, which will be operation-centric and risk-based. What ICAO does with the Standards of Recommended Practices (SARPs) is push them out to the Member States to decide whether they want to adapt the SARPs to their own regulatory framework, or how and why they want to deviate from the SARPs.

On the international level, that process is underway. ICAO will draw a lot from what is happening in the United States, and what is happening in the European Aviation Safety Agency, which is the European equivalent of FAA. Then here, with the states, I think there's going to be a back-and-forth on this sort of model legislation issue, largely because issues related to aviation—especially if they have to do with any sort of safety—will likely be preempted. So, while you might see model legislation for privacy issues or for land use issues, like from where you can land and deploy drones, it's pretty unlikely that you'll see model legislation on particular safety issues or on issues like encryption because a lot of that is going to be driven at the federal level.

Amanda Essex: One thing I'd add to that is while we have seen 49 states consider legislation—and, as I mentioned, 32 have enacted laws—a lot of those have been in areas where FAA has said states have the power to do this. Now, we have Part 107, and states have a better idea of what the feds are doing. I think a lot of states have waited to see what was going to come before they took too much action. So, I think it will be interesting to see what happens in the next legislative session now that we have Part 107.

Joanna Simon: That is a very good point. Another question came in about the examples of drones being used for environmental monitoring or mapping. Can anyone provide other examples where people have used them for things like air sampling, visual or infrared observation, or tracking effluent or emissions?

Joseph Muhlhausen: Yes, you have many applications outside of environmental mapping applications. You have a series of sensors that are small enough to fit into drones that have gas, pressure, or temperature sensors. They have been used for weather forecasting, but have also been used in the case of pipeline leaks. You could sniff out the gas using a drone flying over the pipeline.[29]

Joanna Simon: Thanks. Another question: Are there any gaps in liability law that would hold drone operators or owners liable for damages that their drones would cause? A lot of how liability is going to be allocated will depend on the contracts between operator and manufacturer and pilot, or even software agreements. For example, if you have a software application on your drone that you're going to be using for purposes of monitoring, the terms of service on that app are likely going to allocate liability between the operator, the software manufacturer, and the hardware manufacturer.

If your drone winds up crashing and causing property damage, I would not be surprised if every entity down the line related to that operation is named in the complaint. If the damage is significant, it'll probably name the pilot, the operator, the software writer, and the hardware manufacturer. In other words, everyone in the distribution chain of that drone will likely be named in the complaint.

One thing to think about, which Amanda brought up, is insurance. You always want to make sure you are professionally insured in relation to your drone and your

29. For more information on applications in the oil and gas sector, see Satterlee, *supra* note 2.

drone operation. Aircraft, aviation, and drones are outside general liability coverage. You're going to need to seek out a specific policy related to the drone or have your drone specifically added into your general liability coverage. So, before you start an extensive operation, you should analyze what types of insurance are available, what you have, and how much coverage you think you will need. Amanda, anything you'd like to add to that?

Amanda Essex: I will mention that we do have a section on insurance in our report, and State Farm Insurance was one of our partners on that. The information included on insurance was also reviewed and modified based on the information from State Farm. So, I would certainly recommend checking out that section of our report.

Joanna Simon: Thanks. The next question is primarily for Jeramie. What standard should FAA use to determine if the benefit of improved environmental monitoring exceeds the risk, or even infringement of privacy, that may be concurrent with that monitoring?

Jeramie Scott: I think the standard that can be used is what the court uses in terms of a reasonable expectation of privacy, which looks at whether there are individuals that actually have a reasonable, subjective expectation of privacy, and whether society actually recognizes that or is willing to recognize that expectation of privacy. Again, in the environmental monitoring context, the risks are generally lower, from my understanding and in terms of my familiarity with what environmental monitoring typically consists of. But where there are people or in more-populated areas, the risk increases in terms of collecting personal information or uniquely identifying information on individuals. You run into situations where people have a greater expectation of privacy. It doesn't necessarily mean you can't operate in that area, but it probably does mean that steps need to be taken to provide necessary transparency and ensure the necessary practices.

Joanna Simon: Thanks very much. As a follow-up, some of our listeners are curious about evidentiary requirements. If, for example, a governmental entity used a drone to do environmental monitoring to determine whether an entity is complying with environmental laws, is that okay? Would the government need a warrant, and would it depend on whether the entity has a permit?

Jeramie Scott: Some of that falls outside of my expertise, but I do know in terms of using information collected via drone for some type of evidence, there will be chain-of-custody issues. I see this in the context of another issue that I work on with body cameras. With video collected, whether it is by body cameras or drones, there must be some type of chain-of-custody process that ensures the information collected hasn't been corrupted or modified in some manner that may undermine its use as evidence.

In terms of whether the government needs a warrant, as we heard earlier, a number of states have passed laws in that regard, and some of those laws specify that law enforcement will need a warrant. Warrants are generally to use drones in particular instances, but part of that is going to depend on how the drone is being used. Flying a drone generally over a public area is somewhat of a gray area, but will probably not need a warrant. In contrast, if there is a specific surveillance on an individual that includes following someone as they enter private spaces, you will probably need a warrant, particularly if you're doing that for long periods of time. If the length of time increases, it raises the expectation of privacy.

We saw this in the context of the U.S. Supreme Court case *United States v. Jones*, which was a Global Positioning System (GPS) monitoring case that was actually decided on trespass grounds.[30] One of the concurring opinions talked about this collection of data over a length of time and how that was invasive of privacy. There is an inkling there that the Supreme Court would agree that, even if you don't have a trespass, if you are collecting information on someone's movements in public spaces, then that would require a warrant.

Joanna Simon: I agree with Jeramie, I don't think a warrant would be required for law enforcement to use a drone, unless it's going to be a pretty specific invasion or a long-term ongoing investigation into one person or particular operation. For example, if you're following a car or a person around for weeks at a time, because the drone would make that so much easier than just having a human surveil that person, you would probably need a warrant. However, if you are just monitoring something outside that could be done by one flyover with a helicopter, it might not require a warrant in the same manner.

We have another question: Do FAA regulations apply below certain heights? Yes, the regulation applies regardless of where you are in the airspace. Class G airspace is generally considered uncontrolled airspace. Below 400 feet is mostly going to be Class G, and so Part 107 would apply to that airspace. Therefore, you're going to want to make sure that you're in full compliance with the requirements of the regulation. So, if you're in Class G, you don't need to contact your local ATC tower to let them know about your operation. Yet, if you're in another class or airspace, for example closer to an airport or a helipad, you may need to contact ATC, just to let them know what you're doing.

For example, some large solar sites are set up relatively close to airport property. If you want to use a drone to monitor what's happening at the solar site or to do inspection on the land before you build, you might need to be in direct contact with ATC and the airport to get permission before you launch your drone into the air.

The next question is: What are the export control and International Traffic in Arms Regulations (ITAR) concerns that users should be aware of when using drones?

30. United States v. Jones, 132 S. Ct. 945 (2012).

This is outside of what I generally do, but I can tell you that there are significant export controls on ITAR issues, especially if you are going to go in and out of the United States and in and out of other countries. Drones are considered ITAR-controlled technology. You also need to think about not just the hardware, but also the software and the knowledge. All of that is export-controlled. It's a very particular area of law. If you have concerns about ITAR export control, I would definitely recommend bringing in somebody who has a specialty in that because there are significant issues related to moving drones across borders.

Joseph Muhlhausen: I can talk about my experience with this, because we travel internationally and have called the export control regulation body, the Bureau of Industry and Security. Basically, what they told us is that we have a model that meets the characteristic that I described at the beginning: a drone that contains low-technology consumer goods, but has an Export Control Classification Number. You must travel with it at all times. You cannot ship your drone separately via United Parcel Service. You can check it if you're flying, but it has to remain with you. This is allowed under the "tool of trade" rule. I don't think many companies follow those guidelines right now, but this is the rule when you purchase a drone in the United States and travel abroad for work.

Joanna Simon: Thanks for that insight. That's my understanding as well. We just got another question: Are ATC facilities equipped to handle the types of notices that were just mentioned? Based on my experiences with various clients, if you are going to be flying it across airspace that requires ATC notice, we recommend that you also loop in the local Flight Standards District Office (FSDO). Once you develop a relationship with your local FSDO, they can really help guide you through the notice that's required to airports and ATCs. The FSDO, in combination with the airport and ATC, should be equipped to handle your type of operation.

The good news for environmental monitoring is that you can plan out what you want to do well in advance, for the most part. Sometimes, you may have emergency issues where you would want to get something out there right away, but for monitoring-type operations, you have sufficient leeway to plan and get the necessary authorization from various entities. I encourage everyone to look up their local FSDO on the FAA website, if you don't already know them.

I would also encourage people to check out the apps available for your drone. You can download them onto your iPad, phone, or however you are operating your drone. They will inform you of "no-fly zones," or advise you to be cautious in areas that require drone operators to provide notification and receive authorization before flying. Airspace issues are very complicated, so the more information you have on them before you conduct your operation, the better.

Another question: To resolve trespass claims, do state laws establish property boundary heights vertically above the ground or otherwise?

Amanda Essex: I know a few states have looked at that and have taken action to address it, but I think it is also a question of how much states can really do when you're talking about the airspace. That gets into FAA's territory and preemption. Even though it's trespass, there is this line as to who has the authority there.

Jeramie Scott: In terms of a vertical trespass, what the Supreme Court has said in this area leaves the vertical height for a trespass murky. The Court has not set a level that if you go below, then it instantly becomes a trespass. So, where states have not specified the height at which, for example, a drone trespasses on your property, there is a gray area at what specific level a vertical trespass occurs.

Amanda Essex: As an example, legislation passed in Nevada says that a property owner may sue for trespass against a UAS operator who flies at a height of less than 250 feet above their property, if they've done this before and the property owner has told them not to.[31] Oregon also allows a civil suit under similar conditions with a height requirement of 400 feet.[32] So, a couple of states have taken action on that issue.

Joanna Simon: My last takeaway is that I would encourage everyone who wants to use drones to take a look at Part 107. You will see that the regulatory burden has been significantly reduced and that the cost of using the technology is going to be pretty low. Even if you are not sure how to use a drone at this point, or what kind of return on your investment you will get, it is still going to be a pretty low investment and you might find that drones are a very beneficial technology to get started with.

31. Nev. S.B. 239 (2015).
32. Or. H.B. 2710 (2013).